**Safety and Security Assurance - Extensions to iCMM and CMMI**

*Linda Ibrahim, Co-Project Manager, Federal Aviation Administration*

*3 October 2003*

**Project Description:** The Federal Aviation Administration (FAA) and the Office of the Under Secretary of Defense (OSD) are sponsoring a joint effort with the objective of identifying best safety and security practices for inclusion in the two integrated CMMs: FAA-iCMM v2.0, and CMMI V1.1.

**Why is it important:** Safety and security are critical to DoD and FAA, as well as other government and industry organizations. Both iCMM and CMMI provide process improvement frameworks in which safety and security activities can take place. Yet some practices specific to safety and security are not necessarily addressed in these models. The FAA approved a project to include both safety and security in the iCMM, and the CMMI Steering Group had discussed addressing safety and security. In light of similar needs, FAA and DoD decided to collaborate on developing safety/security extensions to both iCMM and CMMI, the intent being that common content would be included in both models.

**Who is involved:** This project is being co-managed by FAA Chief Engineer for Process Improvement and OSD (AT&L) Defense Systems Directorate, Deputy Director for Software Intensive Systems, with broad participation from government and industry. The team comprises over 30 participants from FAA, OSD, Army, Navy, Air Force, NASA, Department of Energy, Australian Defence Materiel Organization, Defense Contract Management Agency, Software Engineering Institute, Northrup Grumman, Lockheed Martin, Computer Sciences Corp., Harris Corp., I-Metrics, Praxis Critical Systems (UK), and SAIC.

**What produced so far:**

- Selection of Source Material to be integrated and incorporated comprising 3 safety standards and 4 security standards. *For Safety:* MIL-STD-882C: System Safety Program Requirements; IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Systems; DEF STAN 00-56: Safety Management Requirements for Defence Systems. *For Security:* ISO 17799: Information Technology – Code of practice for information security management; ISO 15408: The Common Criteria (v2.1) Mapping of Assurance Levels and Families; Systems Security Engineering CMM (SSE-CMM) (v2.0); NIST 800-30: Risk Management Guide for Information Technology Systems
- Development of integrated practices for safety, and integrated practices for security, combining material from the sources and retaining mappings of all synthesized practices to the source material.
- Harmonization of the safety and security components resulting in combined practices (with mappings retained) that were distributed for external review.
- Disposition of over 200 comments received from ~35 reviewers from US, Australia, and various European countries.
- Draft packaging of reviewed/revised practices into an appropriate form for integration with the existing practices of the reference models
- Two pilot appraisals initiated in the FAA, one to be initiated at Lockheed Martin, one may be initiated in Department of Energy..

**What will be produced in FY04:**

- Final packaging of the harmonized safety and security practices for integration with iCMM and CMMI, including a report describing the project, guidelines for intended use of the application for process improvement and appraisal including evaluation of suppliers, consolidated safety and security glossary, and detailed mapping tables to the source documents.
- Distribution of package for review
- Revision/finalization of final package based on reviewers' comments and pilot appraisal results
- Incorporation into iCMM v2.0 *(Incorporation into CMMI may not necessarily occur in FY04 - tbd)*

**Who will use it:**

In the FAA it is expected that these practices will be utilized: strategically to support on-going cross-agency safety and security work; in any FAA program/organization that deals with safety and security assurance of products and services; by those groups responsible for a safe and secure work environment for the FAA; and by acquisition programs in evaluating the capability of suppliers regarding their safety and security processes and practices. In those organizations that have participated in this project, we anticipate similar usage. In other organizations that use iCMM and CMMI, we anticipate adoption if their business needs include safety and security assurance.